Remarks

In view of the above amendments and the following remarks, reconsideration of the rejection and further examination are requested.

Initially, the Applicants would like to thank the Examiner for conducting the personal interview on June 8, 2006. It is noted that the current amendments to the claims are the same as those proposed during the interview which distinguished the present invention, as recited in the claims, from the references relied upon in the rejection discussed below.

Claims 38-40 have been canceled without prejudice or disclaimer to the subject matter contained therein.

Claims 34, 36 and 37 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Sogabe (US 6,611,534) in view of Ishiguro (US 5,917,910).

Claims 34, 36 and 37 have been amended so as to further distinguish the present invention from the references relied upon in the rejection. As a result, the above-mentioned rejection is submitted to no longer be applicable to the claims for the following reasons.

Claim 34 is patentable over the combination of Sogabe and Ishiguro, since claim 34 recites an information recording medium for recording scrambled data from a recording device including scrambled key information, the information recording medium including, in part, cipher key information that is scrambled and prestored on the information recoding medium and the scrambled data obtained by scrambling contents data using the scrambled key information, wherein the scrambled key information is generated in the recording device from at least the cipher key information that is read from the information recording medium and unscrambled by the recording device, and copy control information. The combination of Sogabe and Ishiguro fails to disclose or suggest the information recording medium including the cipher key information that is scrambled and prestored on the information recording medium and the generation of the scrambled key information from at least the cipher key information that is read from the information recording medium and unscrambled by the recording medium, and the copy control information, as recited in claim 34.

Sogabe discloses a system for storing contents on a recording medium as enciphered data. In the system, a set-top-box (STB) 12 and a DVD-RAM device (DRD) 116 authenticate each other.

The DRD 116 then deciphers an enciphered control key (eKcontrol) sent from the STB 12 to generate a control key (Kcontrol). The STB 12 next sends an enciphered contents key (eKcontent) to the DRD 116 together with enciphered digital contents. The enciphered digital contents contain copy control data (CGMS). The DRD 116 generates a contents key (Kcontent) from the eKcontent using Kcontrol and CGMS. The Kcontent is capable of deciphering the enciphered digital contents. The DRD 116 then records the enciphered digital contents directly on the recording medium and records the corresponding Kcontent and the CGMS in a gap area of the recording medium. (See column 8, lines 10 and 11 and column 9, lines 27-54).

Based on the above discussion of Sogabe, the DRD 116 receives both the control key and the contents key from the STB 12 in enciphered form. The DRD 116 is able to decipher the control key and then use the control key to decipher the contents key. The contents key, which is capable of deciphering the enciphered digital contents, is then recorded on the recording medium with the enciphered digital contents. In comparing the disclosure of Sogabe with the invention as recited in claim 34, it is apparent that the two are quite different.

Since the control key is used to decipher the contents key in Sogabe, the control key can be said to correspond to the claimed cipher key information, which is used to generate the scrambled key information. Further, since the contents key in Sogabe is used to decipher the scrambled data, the contents key can be said to correspond to the claimed scrambled key information, which is used to obtain the scrambled contents data. However, claim 34 recites that the cipher key information is scrambled and prestored on the information recording medium and that the cipher key information is read from the information recording medium and unscrambled by the recording device to be used to generate the scrambled key information. Therefore, in order for Sogabe to disclose or suggest this feature, the control key would have to be scrambled and prestored on the recording medium, and then read from the recording medium and unscrambled by the DRD 116 to be used to decipher the contents key. Based on the above discussion of Sogabe, the system disclosed therein clearly does not operate in this manner. Instead, the contents key, not the control key, is stored on the recording medium. Further, the control key would also have to be scrambled (i.e., enciphered) and prestored on the recording medium in order to meet the limitations of the claimed cipher key information, which features are not disclosed or suggested with respect to the control key. As a result, it is

necessary for Ishiguro to disclose or suggest these features in order for the combination of Sogabe and Ishiguro to render claim 34 obvious.

Regarding Ishiguro, it discloses an encrypting apparatus 1 that encrypts information prior to saving the information on a recording medium. The encrypting apparatus 1 includes an inherent information generating unit 5 that outputs information which is inherent in a recording medium. The encrypting apparatus 1 generates an encryption key based on the inherent information from the inherent information generating unit 5 and encrypts the information with the encryption key. The encrypted information is then stored on the recording medium. Further, the inherent information is also stored as an unencrypted file on a predetermined region of the recording medium. The inherent information can be extracted from the recording medium by an authorized device and used to create the decryption key needed to decrypt the encrypted data. The inherent information is described as being a normal file that can be copied. However, unauthorized copying of the recording medium is prevented because such unauthorized copying results in the position of the inherent information being changed. This change of position prevents the proper creation of the decryption key, which prevents the encrypted information from being decrypted. (See column 1, line 65 - column 2, line 5 and column 4, lines 1-23).

As indicated in the rejection, Ishiguro does disclose that the inherent information, which is stored on the recording medium, is used to generate the encryption key used to encrypt information to be stored on the recording medium. However, as discussed above, the inherent information is in no way scrambled and prestored on the recording medium. Instead, the encrypting apparatus 1 generates the inherent information (via the inherent information generating unit 5) and the encrypted information, which is encrypted based on the inherent information, during the same writing session and writes both to the recording medium. Therefore, the encryption key of Ishiguro cannot be said to be generated in the encrypting apparatus 1 from scrambled and prestored information which is read from the recording medium and unscrambled by the encrypting apparatus 1. As a result, it is clear that Ishiguro also fails to disclose or suggest these features.

In consideration of the above discussion, Sogabe and Ishiguro do not, either alone or in combination, disclose or suggest an information recording medium including, in part, cipher key information that is scrambled and prestored on the information recoding medium and scrambled data

obtained by scrambling contents data using the scrambled key information, wherein the scrambled key information is generated in a recording device from at least the cipher key information that is read from the information recording medium and unscrambled by the recording device, and copy control information. Therefore, one of ordinary skill in the art would not have been motivated to modify or combine the references so as to obtain the invention as recited in amended claim 34. Accordingly, it is respectfully submitted that amended claim 34 is clearly patentable over the prior art of record.

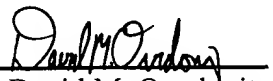
As for claims 36 and 37, they are patentable over the references for reasons similar to those set forth above in support of claim 34. That is, claims 36 and 37 recite, in part, the reading and descrambling of cipher key information that is scrambled and prestored on an information recording medium from the information recording medium to a recording device for creating scrambled content data, which feature is not disclosed or suggested by the references.

Because of the above-mentioned distinctions, it is believed clear that claims 34, 36 and 37 are allowable over the references relied upon in the rejections. Furthermore, it is submitted that the distinctions are such that a person having ordinary skill in the art at the time of invention would not have been motivated to make any combination of the references of record in such a manner as to result in, or otherwise render obvious, the present invention as recited in claims 34, 36 and 37. Therefore, it is submitted that claims 34, 36 and 37 are clearly allowable over the prior art of record.

In view of the above amendments and remarks, it is submitted that the present application is now in condition for allowance. The Examiner is invited to contact the undersigned by telephone if it is felt that there are issues remaining which must be resolved before allowance of the application.

Respectfully submitted,

Takashi YUMIBA et al.

By: 

David M. Ovedovitz
Registration No. 45,336
Attorney for Applicants

DMO/jmj
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
June 26, 2006